

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA**

JACQUELYN HEISERMAN,
Individually, and on Behalf of All Others
Similarly Situated,

Plaintiff,

Case No. 23-cv-297

V.

MATERNAL AND FAMILY
HEALTH SERVICES, INC.

Defendant.

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Jacquelyn Heiserman (“Plaintiff”), through her undersigned counsel, brings this action against Maternal and Family Health Services, Inc. (“MFHS” or “Defendant”) pursuant to the investigation of her attorneys, personal knowledge as to herself and her own acts and otherwise upon information and belief, and alleges as follows:

INTRODUCTION

1. MFHS is a “non-profit health and human services organization” which oversees a network of health and nutrition centers throughout Eastern Pennsylvania.

2. On or about April 4, 2022, Defendant learned that it was the victim of a hack and exfiltration of Sensitive Personal Information (“SPI”) that occurred between August 21, 2021 and April 4, 2022. According to notice provided to the Maine Attorney General, the total number of individuals affected was 461,070.¹

¹ See <https://apps.web.maine.gov/online/aeviewer/ME/40/aa8282f5-0293-41fe-8074-d62e568e05ac.shtml> (last accessed January 23, 2023).

3. MFHS reported that this SPI included at least names, addresses, dates of birth, Social Security numbers, driver's license numbers, financial account/payment card information, usernames and passwords, medical information and/or health insurance information.²

4. Plaintiff and Class members now face a present and imminent lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

5. The information stolen in cyber-attacks allows the modern thief to assume victims' identities when carrying out criminal acts such as:

- Filing fraudulent tax returns;
- Using the victim's credit history;
- Making financial transactions on behalf of victims, including opening credit accounts in victims' names;
- Impersonating victims via mail and/or email;
- Impersonating victims in cyber forums and social networks;
- Stealing benefits that belong to victims; and
- Committing illegal acts which, in turn, incriminate victims.

6. Plaintiff's and Class members' SPI was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the SPI of Plaintiffs and Class members.

7. As of this writing, there exist many class members who have no idea their SPI has been compromised, and that they are at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

8. Plaintiff brings this action on behalf of all persons whose SPI was compromised as a result of Defendant's failure to: (i) adequately protect consumers' SPI, (ii) adequately warn its

² See <https://www.mfhs.org/important-information-about-maternal-family-health-services-2022-cybersecurity-incident/> (last accessed January 23, 2023)

current and former customers and potential customers of its inadequate information security practices, and (iii) effectively monitor its platforms for security vulnerabilities and incidents (the “Class”). Defendant’s conduct amounts to negligence and violates state statutes.

9. Plaintiff and similarly situated individuals have suffered injury as a result of Defendant’s conduct. These injuries include: (i) lost or diminished inherent value of SPI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their SPI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) deprivation of rights they possess under California Confidentiality of Medical Information Act; and (v) the continued and certainly an increased risk to their SPI, which remains in Defendant’s possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the SPI.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

11. This Court has personal jurisdiction over Defendant because Defendant’s maintains offices in this district and does business within this district.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant resides within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

PARTIES

13. Plaintiff Jacquelyn Heiserman is a natural person residing in Lehigh County, Pennsylvania. On or about January 15, 2023, Plaintiff Heiserman was informed that she had been a victim of the Data Breach.

14. Defendant Maternal and Family Health Services, Inc. is a nonprofit Pennsylvania corporation with its principal place of business at 15 Public Square, Wilkes-Barre, Pennsylvania.

FACTUAL ALLEGATIONS

15. Defendant is a not-for-profit health and human services organization with 12 offices in Eastern Pennsylvania. Defendant's operations include medical examinations and treatments at its offices.

16. Defendant sees at least thousands of patients and clients a year at its offices.

17. In the ordinary course of doing business with Defendant, patients provide Defendant or with SPI such as:

- a. Contact and account information, such as name, usernames, passwords, address, telephone number, email address, and household members;
- b. Authentication and security information such as government identification, Social Security number, security codes, and signature;
- c. Demographic information, such as age, gender, and date of birth;
- d. Payment information, such as credit card, debit card, and/or bank account number; and
- e. Medical history as self-reported by patients, or medical history as transmitted from other healthcare providers;

18. On or about January 10, 2023, Defendant announced publicly that on April 4, 2022, that it “was made aware of a sophisticated ransomware incident that may have resulted in the inadvertent exposure of sensitive information to an unauthorized individual.”³

19. Of concern, while Defendant became aware of the Data Breach no later than April 4, 2022, it took more than eight months for Defendant to notify patients, clients, and the media of the breach.

20. As a result, Plaintiff’s and class members’ SPI was in the hands of hackers for approximately somewhere between eight and sixteen months before Defendant began notifying them of the Data Breach.

21. Defendant has been extremely vague on its response to the Data Breach, stating only that it is “committed to strengthening our systems’ security to prevent this kind of incident from happening again.”⁴

22. As of this writing, Defendant has offered no detailed information on the steps it has taken or specific efforts made to reasonably ensure that such a breach cannot or will not occur again.

23. This response is entirely inadequate to Plaintiff and class members who now potentially face several years of heightened risk from the theft of their SPI and who may have already incurred substantial out-of-pocket costs in responding to the Data Breach.

24. MFHS bills itself as a company with a “[c]ommitment to quality in our work and to the respect and dignity for the individuals we serve.”⁵

³ *Id.*

⁴ *Id.*

⁵ See <https://www.mfhs.org/about-us/our-values/>, last accessed January 23, 2023.

25. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class members, to keep their SPI confidential and to protect it from unauthorized access and disclosure.

26. Plaintiff and Class members provided their SPI to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

27. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the industry preceding the date of the breach.

28. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

29. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.⁶ Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.⁷

⁶ See *Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), <https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf>, last accessed January 23, 2023.

⁷ The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

30. The SPI of Plaintiff and members of the Classes was taken by hackers to engage in identity theft and/or to sell it to other criminals who will purchase the SPI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

31. Defendant knew, or reasonably should have known, of the importance of safeguarding the SPI of Plaintiff and members of the Class, including Social Security numbers, dates of birth, and other sensitive information, as well as of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and members of the Class as a result of a breach.

32. Plaintiff and members of the Class now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their SPI.

33. The injuries to Plaintiff and members of the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the SPI of Plaintiff and members of the Class.

34. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

35. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone

is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

36. The FTC further recommends that companies not maintain SPI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

37. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

38. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer SPI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

39. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant’s cybersecurity practices.

40. Best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

41. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7,

PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

42. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

43. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

44. The SPI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.⁸

45. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought.

⁸ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, (Oct. 16, 2019), <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs>, last accessed January 23, 2023.

Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.⁹

46. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

47. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, “The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”¹⁰

48. Furthermore, as the SSA warns:

Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

If you receive a new Social Security Number, you should not be able to use the old number anymore.

For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.¹¹

⁹ SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), <https://www.ssa.gov/pubs/EN-05-10064.pdf>, last accessed January 23, 2023.

¹⁰ Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft>, last accessed January 23, 2023.

¹¹ SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), <https://www.ssa.gov/pubs/EN-05-10064.pdf>, last accessed January 23, 2023.

49. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential SPI to mimic the identity of the user. The personal data of Plaintiff and members of the Class stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiff and the Class. Stolen personal data of Plaintiff and members of the Classes represents essentially one-stop shopping for identity thieves.

50. The FTC has released its updated publication on protecting SPI for businesses, which includes instructions on protecting SPI, properly disposing of SPI, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

51. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office (“GAO”) Report to Congressional Requesters:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.¹²

52. Companies recognize that SPI is a valuable asset. Indeed, SPI is a valuable commodity. A “cyber black-market” exists in which criminals openly post stolen Social Security numbers and other SPI on a number of Internet websites. The stolen personal data of Plaintiff and members of the Class has a high value on both legitimate and black markets.

53. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver license or identification card in the victim’s name but with another’s picture, and/or using the victim’s information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years

¹² See <https://www.gao.gov/assets/gao-07-737.pdf> (June 2007) at 29, last accessed January 23, 2023.

for identity theft to come to light and be detected.

54. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendant's former and current customers whose Social Security numbers have been compromised now face a real, present, imminent and substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

55. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, driver license number or government-issued identification number, name, and date of birth.

56. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."¹³

57. Among other forms of fraud, identity thieves may obtain driver licenses, government benefits, medical services, and housing or even give false information to police. An individual may not know that his or her driver license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

¹³ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>, last accessed January 23, 2023.

FACTS SPECIFIC TO PLAINTIFF

58. On or about January 15, 2023, Plaintiff was notified via a letter from Defendant that she had been a victim of the hack.

59. Plaintiff was a patient of Defendant most recently in 2006. In fact, Defendant did not send the notice letter to Plaintiff at her current address – she was informed by a friend at her former place of work that she had received a notice letter.

60. In spite of the fact that Plaintiff has not been a patient of Defendant for more than 15 years, Defendant still had Plaintiff's SPI on file in its systems.

61. Had Plaintiff known that her SPI would not have been adequately protected by Defendant, she would not have used Defendant's services or she would have insisted that they not be stored in Defendant's system.

62. In January 2023, Plaintiff received several fraudulent charges on her American Express card related to the purchase of infant formula and supplies.

63. Additionally, Plaintiff is aware of no other source from which the theft of her SPI could have come. She regularly takes steps to safeguard her own SPI in her own control. At minimum, Plaintiff believes that the hackers were able to use her SPI stolen from Defendant in order to gain access to her American Express account.

64. Since the time of the Data Breach, Plaintiff has experienced an increase in the number of spam calls, texts, and emails related to medical procedures. This activity indicates that her information has been placed into the hands of hackers and has already been sold throughout the dark web.

CLASS ACTION ALLEGATIONS

65. Plaintiff brings this nationwide class action pursuant to Rules 23(b)(2), 23(b)(3),

and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following classes:

All natural persons residing in the United States whose SPI was compromised in the Data Breach announced by Defendants on or about January 10, 2023 (the “Class”).

66. Excluded from the Class are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

67. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

68. **Numerosity:** The Class is so numerous that joinder of all members is impracticable. Defendant has indicated that the total number of Class Members is 461,070. The Class is readily identifiable within Defendant’s records.

69. **Commonality:** Questions of law and fact common to the Class exist and predominate over any questions affecting only individual members of the Class. These include:

- a. When Defendant actually learned of the Data Breach and whether its response was adequate;
- b. Whether Defendant owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their SPI;
- c. Whether Defendant breached that duty;
- d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the SPI of Plaintiff and members of the Class;
- e. Whether Defendant acted negligently in connection with the monitoring and/or protection of SPI belonging to Plaintiff and members of the Class;
- f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep the SPI of Plaintiff and members of the Class secure and to prevent loss or misuse of that SPI;

g. Whether Defendant has adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendant caused Plaintiff and members of the Class damage;

i. Whether Defendant violated the law by failing to promptly notify Plaintiff and members of the Classes that their SPI had been compromised; and

j. Whether Plaintiff and the other members of the Class are entitled to credit monitoring and other monetary relief.

70. **Typicality:** Plaintiff's claims are typical of those of the other members of the Class because all had their SPI compromised as a result of the Data Breach due to Defendant's misfeasance.

71. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's counsel are competent and experienced in litigating privacy-related class actions.

72. **Superiority and Manageability:** Under rule 23(b)(3) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Individual damages for any individual member of the Class are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

73. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

74. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues

include, but are not limited to:

- a. Whether Defendant owed a legal duty to Plaintiff and members of the Class to exercise due care in collecting, storing, using, and safeguarding their SPI;
- b. Whether Defendant breached a legal duty to Plaintiff and the members of the Class to exercise due care in collecting, storing, using, and safeguarding their SPI;
- c. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and
- e. Whether members of the Class are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

FIRST CLAIM FOR RELIEF

Negligence

(By Plaintiff Individually and on Behalf of the Class)

75. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 73.

76. Defendant routinely handles SPI that is required of their patients and customers, such as Plaintiff.

77. By collecting and storing the SPI of its patients and customers, Defendant owed a duty of care to the individuals whose SPI it collected to use reasonable means to secure and safeguard that SPI.

78. As a medical services provider, Defendant is aware of that duty of care to the SPI of its clients' patients.

79. Additionally, as a covered entity, Defendant has a duty under HIPAA privacy laws to protect the confidentiality of patient healthcare information, including the kind stolen as part of the Data Breach.

80. Defendant has full knowledge of the sensitivity of the SPI and the types of harm that Plaintiffs and Class Members could and would suffer if the SPI were wrongfully disclosed.

81. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of their current and former employees' SPI, and that of their beneficiaries and dependents, involved an unreasonable risk of harm to Plaintiffs and Class Members, even if the harm occurred through the criminal acts of a third party.

82. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff's and Class Members' information in Defendant's possession was adequately secured and protected.

83. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' SPI.

84. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

85. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of or should have known of the inherent risks in collecting and storing the SPI of Plaintiff and the Class, the critical importance of providing adequate security of that SPI, and the necessity for encrypting SPI stored on Defendant's

systems.

86. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' SPI, including basic encryption techniques freely available to Defendant.

87. Plaintiff and the Class Members had no ability to protect their SPI that was in, and possibly remains in, Defendant's possession.

88. Defendant was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

89. Defendant had and continues to have a duty to adequately disclose that the SPI of Plaintiff and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their SPI by third parties.

90. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the SPI of Plaintiff and Class Members.

91. Defendant has admitted that the SPI of Plaintiff and Class Members was purposely exfiltrated and disclosed to unauthorized third persons as a result of the Data Breach.

92. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the SPI of Plaintiff and Class Members during the time the SPI was within Defendant's possession or control.

93. Defendant improperly and inadequately safeguarded the SPI of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

94. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect its current and former employees' SPI in the face of increased risk of theft.

95. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former employees' SPI.

96. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

97. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the SPI of Plaintiff and Class Members would not have been compromised.

98. There is a close causal connection between Defendant's failure to implement security measures to protect the SPI of Plaintiff and Class Members and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and Class Members' SPI was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such SPI by adopting, implementing, and maintaining appropriate security measures.

99. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their SPI is used; (iii) the compromise, publication, and/or theft of their SPI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their SPI; (v) lost opportunity

costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their SPI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the SPI of its employees and former employees in its possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the SPI compromised as a result of the Data Breach for the remainder of Plaintiff's and Class Members' lives.

100. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their SPI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the SPI in its continued possession.

SECOND CLAIM FOR RELIEF
Breach of Implied Contract
(By Plaintiff Individually and on Behalf of the Class)

101. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 73.

102. When Plaintiff and Class Members provided their SPI to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant under which—and by mutual assent of the parties—Defendant agreed to take reasonable steps to protect their SPI.

103. Defendant solicited and invited Plaintiff and Class Members to provide their SPI as part of Defendant's regular business practices and as essential to the services transactions entered

into between Defendant on the one hand and Plaintiff and Class Members on the other. This conduct thus created implied contracts between Plaintiff and Class Members on the one hand, and Defendant on the other hand. Plaintiff and Class Members accepted Defendant's offers by providing their SPI to Defendant in connection with their purchases from Defendant.

104. When entering into these implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws, regulations, and industry standards.

105. Defendant's implied promise to safeguard Plaintiff's and Class Members' SPI is evidenced by a duty to protect and safeguard SPI that Defendant required Plaintiff and Class Members to provide as a condition of entering into consumer transactions with Defendant.

106. Plaintiff and Class Members paid money to Defendant to purchase services from Defendant. Plaintiff and Class Members reasonably believed and expected that Defendant would use part of funds received as a result of the purchases to obtain adequate data security. Defendant failed to do so.

107. Plaintiff and Class Members, on the one hand, and Defendant, on the other hand, mutually intended—as inferred from patients' continued use of Defendant's services—that Defendant would adequately safeguard SPI. Defendant failed to honor the parties' understanding of these contracts, causing injury to Plaintiff and Class Members.

108. Plaintiff and Class Members value data security and would not have provided their SPI to Defendant in the absence of Defendant's implied promise to keep the SPI reasonably secure.

109. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

110. Defendant breached its implied contracts with Plaintiff and Class Members by failing to implement reasonable data security measures and permitting the Data Breach to occur.

111. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiff and Class Members sustained damages as alleged herein.

112. Plaintiff and Class Members are entitled to compensatory, consequential, and other damages suffered as a result of the Data Breach.

113. Plaintiff and Class Members also are entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide credit monitoring and identity theft insurance to Plaintiff and Nationwide Class members.

THIRD CLAIM FOR RELIEF

Unjust Enrichment

(By Plaintiff Individually and on Behalf of the Nationwide Class)

114. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 73.

115. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of storing their SPI with Defendant in such a way that saved expense and labor for Defendant.

116. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Defendant also benefited from the receipt of Plaintiff's and Class Members' SPI, as this was used by Defendant to facilitate its core functions.

117. The benefits given by Plaintiff and Class Members to Defendant were to be used by Defendant, in part, to pay for or recoup the administrative costs of reasonable data privacy and security practices and procedures.

118. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount to be determined at trial.

119. Under principles of equity and good conscience, Defendant should not be permitted to retain a benefit belonging to Plaintiff and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members granted to Defendant or were otherwise mandated by federal, state, and local laws and industry standards.

120. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds or benefits it received as a result of the conduct alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all Class Members, requests judgment against the Defendant and the following:

- A. For an Order certifying the Class as defined herein, and appointing Plaintiff and his counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' SPI;
- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

- ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
- iii. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff and Class Members' personal identifying information;
- iv. prohibiting Defendant from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database (if, in fact, it does so);
- v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's

systems;

- ix. requiring Defendant to conduct regular database scanning and securing checks;
- x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

- xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
 - xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and
 - xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and
- D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For pre- and postjudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiff hereby demands a trial by jury on all issues so triable.

DATED: January 24, 2023

Respectfully Submitted,

/s/ Mark C. Rifkin

Mark C. Rifkin

WOLF HALDENSTEIN ADLER

FREEMAN & HERZ LLP

270 Madison Ave.

New York, New York 10016

Tel: (212) 545-4600
Fax: (212) 686-0114
rifkn@whafh.com

Carl V. Malmstrom
(*pro hac vice* forthcoming)
**WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLC**
111 W. Jackson Blvd., Suite 1700
Chicago, Illinois 60604
Tel: (312) 984-0000
Fax: (212) 686-0114
malmstrom@whafh.com

Counsel for Plaintiff and the Putative Class